Document Title	Explanation of IPsec Implementation Guidelines
Document Category	Explanation (EXP)
Document UID	930
Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R26-11

Document Change History

Date	Release	Changed by	Description
2026-11-26	R26-11	AUTOSAR Release Management	• added IKEv2 Post-quantum Security Extension according to IETF RFC 8784
2025-11-27	R25-11	AUTOSAR Release Management	• No content changes
2024-11-27	R24-11	AUTOSAR Release Management	• No content changes
2023-11-23	R23-11	AUTOSAR Release Management	• No content changes
2022-11-24	R22-11	AUTOSAR Release Management	• No content changes
2021-11-25	R21-11	AUTOSAR Release Management	• No content changes
2020-11-30	R20-11	AUTOSAR Release Management	• No content changes • Changed Document Status from Final to published
2019-11-28	R19-11	AUTOSAR Release Management	• No content changes • Changed Document Status from Final to published
2019-03-29	19-03	AUTOSAR Release Management	• No content changes
2018-10-31	18-10	AUTOSAR Release Management	• Initial release

Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

Table of Contents

1 Introduction 4
2 The Basics of IPsec Protocol 5
3 Objective 8
4 Primary recommendations 9
5 Detailed requirements for IPsec implementation 12
6 Further guidance 14
7 Supplementary information 15
8 Related documentation 16
9 Acronyms and Abbreviations 17

1 Introduction

1.1 Scope of this document

This document provides guidelines for IPsec implementation in the AUTOSAR Adaptive Platform.

1.2 Relation to other standards

This document is relevant to AUTOSAR Adaptive Platform only.

2 The Basics of IPsec Protocol

2.1 IPsec protocol - network security standard

IPsec is a network layer protocol suite that secures network connections by encrypting or authenticating IP packets. It constitutes a part of IP protocol suite.

IPsec consists of three elementary components:

- Internet Key Exchange - most widely used module for key management
- Authentication Header - (IP protocol 51) for integrity
- Encapsulating Security Payload - (IP protocol 50) for integrity and confidentiality

It is an open network standard, maintained by IETF since 1995 and commonly used in network equipment as well as server and desktop operating systems.

The IPsec can be implemented in the IP stack of an operating system, which requires modification of the source code. This method of implementation is done for many host and security gateway operating systems.

IPsec works in two basic modes of operation:

- Transport mode
- Tunnel mode

The following drawings explain packet structure of Authentication Header and Encapsulating Security Payload.

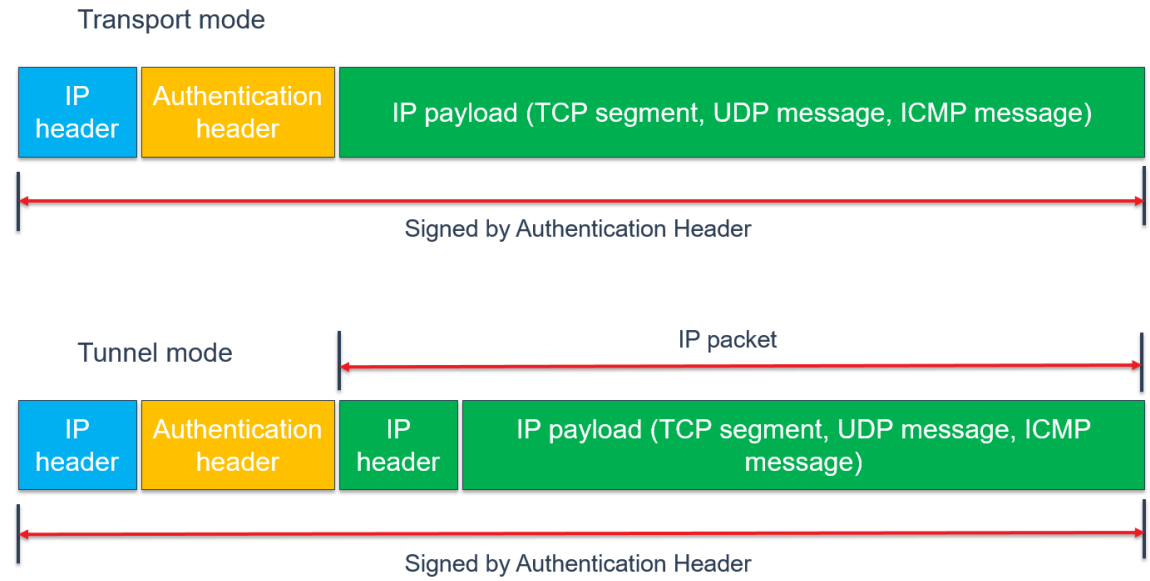


Figure 2.1: Authentication Header (AH) frame

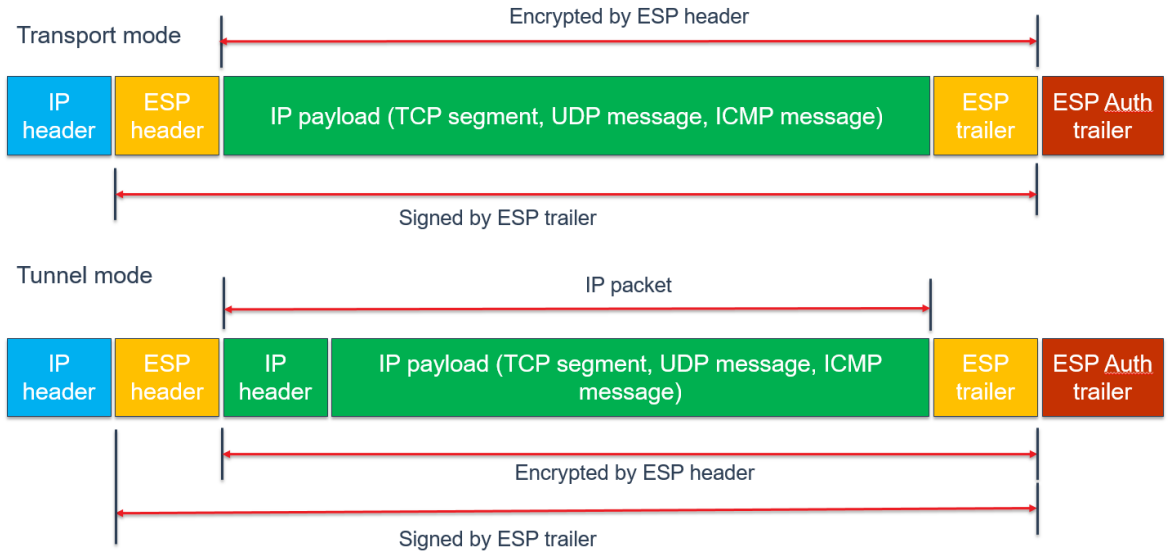


Figure 2.2: Encapsulating Security Payload (ESP) frame

2.2 Internet Key Exchange operation

In order to create session keys necessary for the network traffic protection IKE starts key exchange and stores Security Associations. A Security Association (SA) is the formation of shared security elements between two network nodes in order to support secure communication. It may include attributes such as: cryptographic algorithm and mode, traffic encryption key, and parameters for the network data to be passed over the connection. They are usually stored in Security Associations Database.

Usually, a Security Association consists of at least the following parameters:

- Destination IP address
- Security Parameter Index (SPI)
- IPsec protocol identifier (AH / ESP)
- Mode (transport / tunnel)
- Key and algorithms used
- Lifetime

The following drawing explains the meaning of IKE module, security associations and security policies databases for securing IPsec network communication.

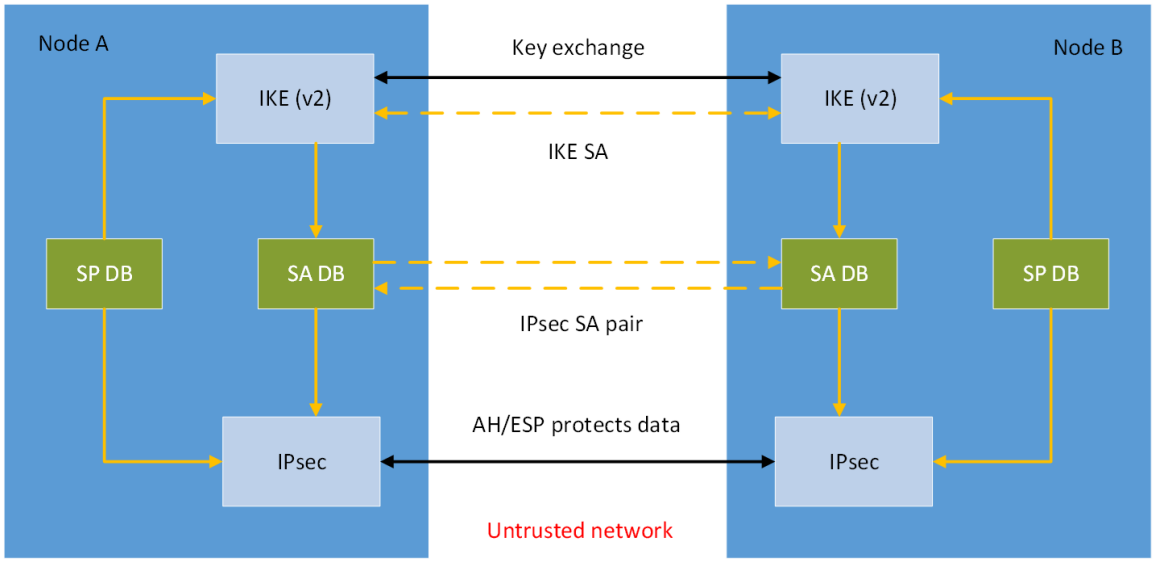


Figure 2.3: SA creation with IKE for network traffic protection

3 Objective

The objective of IPsec protocol implementation in AUTOSAR Adaptive Platform is providing secure communication channels in the in-vehicle IP network.

Implementing IPsec in AUTOSAR Adaptive Platform would provide options for securing communication between network nodes with confidentiality, integrity or both guaranteed.

IPsec, as a standard network security protocol provides means for secure communication, while supporting multi-vendor stack interoperability.

4 Primary recommendations

4.1 Prerequisites

As IPsec is a subset of IP protocol suite and is fully dependent on IP stack functionality, a fully useful IP stack enables IP network packet flow, necessary for IPsec protocol service.

4.2 Implementation of IPsec in AUTOSAR AP stack

Adaptive Platform does not specify any operating system for an Electronic Control Unit (ECU) and as of that, implementing state-of-the-art IPsec functionality along with best practices, it is the stack vendor responsibility.

This goal can be achieved without engaging any higher network stack level, i.e. communication channel established with IPsec would be fully transparent for AUTOSAR Adaptive Platform Communication Management functional cluster, thus for Adaptive Applications as well.

The following picture outlines the design of the AUTOSAR Adaptive stack. The functionality of the stack, presented below Communication Management there, is defined in AUTOSAR Adaptive Platform documentation only in the Specification of Manifest [1], what is represented as 'IKE config' and 'IPsec config' here.

This is only an example, based on Linux architecture and might require some modifications for other operating systems.

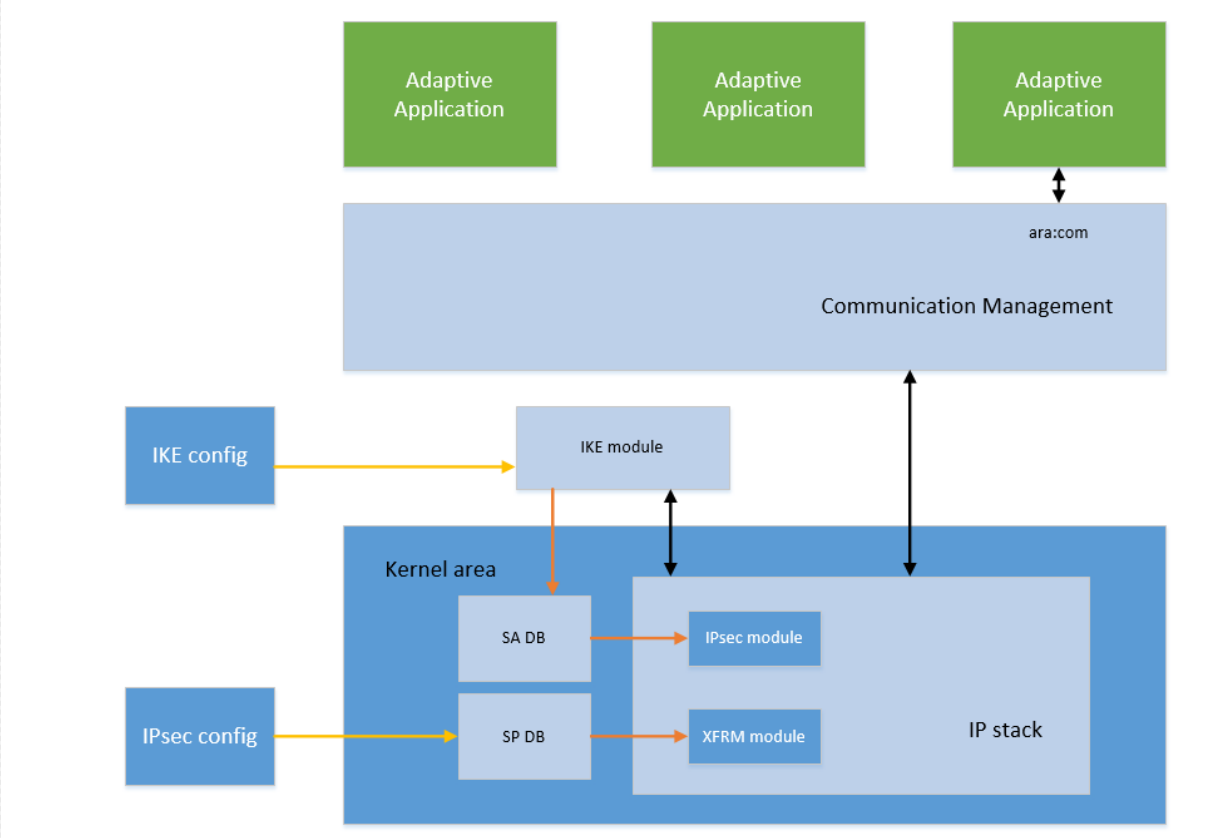


Figure 4.1: Communication with IPsec in AUTOSAR Adaptive Platform

4.3 Operating System kernel with an IP stack

As mentioned above, IPsec requires OS usage of an IP stack, usually located in the kernel area. Being just a subset of the IP protocol suite, and a part of the IP stack in the end, IPsec would need to be integrated with the bare IP stack. That would be routinely obtained with compiling OS kernel along with IP stack and IPsec modules.

4.4 Kernel IPsec module

Most of current operating systems offer modern IP stack modules, extensible with IPsec functionality. They should be applied along with filtering modules (like e.g. the

XFRM Framework in Linux), allowing packet management according to IPsec rules, as described in Specification of Manifest [1].

IPconfig part defined in Specification of Manifest would be typically represented as security policies, forming security policies database, but it depends on implementation in the end.

4.5 IKE module

In order to make IPsec operative an Internet Key Exchange (IKE) module is needed. Typically, it would not be a part of the kernel space and require separated integration.

For AUTOSAR Adaptive Platform IKE version 2 should be used. IKEv2 provides modern security options and is eventually easier to implement.

IKE config would usually stand for a configuration file.

IKE module needs to be initialised during boot process in order to make sure all necessary security associations would be ready before the node starts communication.

5 Detailed requirements for IPsec implementation

While integrating IPsec in AUTOSAR Adaptive Platform, the following requirements should be met. That would ensure compatibility and superior security posture.

- IPsec shall be implemented based on the following standards:
  - Security Architecture for the Internet Protocol "RFC 4301 [2]"
  - Authentication Header (AH) "RFC 4302 [3]"
  - Encapsulating Security Payload (ESP) "RFC 4303 [4]"
- The IPsec implementation shall support Extended Sequence Number "RFC 4304 [5]".
- The implementation shall support these algorithms for AH and use them in this preferences order (highest priority first):
  - AUTH_AES_GMAC: AES Galois Message Authentication Code (GMAC) "RFC 4543 [6]"
  - AUTH_AES_CMAC_96: AES Cipher-based Message Authentication Code (CMAC) "RFC 4494 [7]"
- The following algorithms for ESP shall be supported in this priority:
  - AES-GCM with 16 octet ICV "RFC 4106 [8]"
  - ENCR_AES_CCM_16 "RFC 4309 [9]"
- The IPsec implementation shall support at least Suite-B-GMAC-128 from "RFC 6379 [10]" for both ESP and AH.
- Internet Key Exchange Protocol Version 2 (IKEv2) shall be supported "RFC 7296 [11]".
- The IKEv2 implementation shall support the Post-quantum Security Extension "RFC 8784 [12]".
- The IKEv2 implementation shall support authentication based on X.509v3 Certificates with digital signatures "RFC 7427 [13]".
- IKEv2 shall gracefully shutdown by sending DELETE_SAs on closure and rebuilding them on startup.
- IKEv2 shall use Dead Peer Detection.
- Configuration shall define the rekey interval for SA and child SA.
- The implementation shall support a seamless handover between exchanged keys.
- IPsec implementation shall use the Transport Mode.

- IPsec Tunnel Mode is currently not supported.
- The following ports shall be not protected by IPsec:
  - 500/UDP: IKEv2 packets
  - 4500/UDP: IKEv2 packets
  - 6801/TCP: Diagnostics

6 Further guidance

6.1 Multicast communication

Multicast communication secured with IPsec is currently not planned for AUTOSAR Adaptive Platform, what simplifies key management and reduces the risk of a key disclosure.

These benefits for smaller networks, like in-vehicle network, would usually prevail.

6.2 Retry for key update

If the peer ECU is not available when keys shall be updated, the ECU retries, whether the peer ECU is available again. That way security association can be obtained despite a temporary node unavailability.

6.3 Backward Compatibility

Electronic Control Units with IPsec support shall allow integration into vehicles, in which their communication partners do not support IPsec. Configuration options for either IP or IPsec communication for specific peers shall be available.

6.4 Filtering with IPsec rules

The ECU shall support that certain application sockets - IP address, protocol, and port number - can only be connected using IPsec.

6.5 Patch Management

It is highly recommended to check, if there is an update available for libraries integrated in the IPsec kernel module or IKE module, and apply them whenever possible.

6.6 Security Functions Development

When there is a new cryptographic function available, like e.g. new encryption algorithm, it would make sense to introduce it. It would work reasonable, however, only when performed based on approved RFC documents.

7 Supplementary information

The above mentioned requirements should not be regarded as exhaustive, and the final implementation does not need to be restricted to them.

In particular, documentation specific to software packets picked out for integration with the operating system stack should be taken into consideration.

8 Related documentation

[1] Specification of Manifest
AUTOSAR_AP_TPS_ManifestSpecification

[2] RFC 4301, Security Architecture for the Internet Protocol

[3] RFC 4302, IP Authentication Header

[4] RFC 4303, IP Encapsulating Security Payload (ESP)

[5] RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association

[6] RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH

[7] RFC 4494, The AES-CMAC-96 Algorithm and Its Use with IPsec

[8] RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)

[9] RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)

[10] RFC 6379, Suite B Cryptographic Suites for IPsec

[11] RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2)

[12] RFC 8784, Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

[13] RFC 7427, Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)

9 Acronyms and Abbreviations

The glossary below includes acronyms and abbreviations relevant to the explanation of IPsec implementation in AUTOSAR Adaptive Platform.

Abbreviation / Acronym:	Description:
AH	Autenticating Header protocol
DB	Database
ECU	Electronic Control Unit
ESP	Encapsulating Security Payload protocol
IKE	Internet Key Exchange protocol
IP	Internet protocol
IPsec	Internet Protocol Security protocol
SA	Security Association